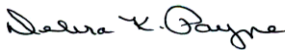
 <p style="text-align: center;">POLICIES AND PROCEDURES</p> <p style="text-align: center;">State of Tennessee Department of Intellectual and Developmental Disabilities</p>	Policy #: 80.4.4	Page 1 of 5
	Effective Date: April 1, 2016	
	Distribution: B	
Policy Type: Community Waiver	Supersedes: 80.4.4 (8/10/12), P-022	
Approved by:  Debra K. Payne, Commissioner	Last Review or Revision: November 18, 2015	
Subject: ELECTRONIC RECORDS AND SIGNATURES		

- I. **AUTHORITY:** Electronic Signatures in Global and National Commerce Act, "Consumer Consent Provision" Section 101(c)(1)(C)(ii); Health Insurance Portability Accountability Act (HIPAA) of 1996; Section 1915(c) of the Social Security Act (Medicaid Waivers); Tennessee Code Annotated (TCA) 4-3-2708, TCA 33-3-101, TCA 33-1-302(a), TCA 33-1-303, TCA 33-1-305, TCA 34-8-502, and TCA 47-10-107.
- II. **PURPOSE:** The purpose of this policy is to define general requirements for the acceptable use of electronic records and electronic signatures by contracted providers of the Department of Intellectual and Developmental Disabilities (DIDD) including Home and Community Based Services (HCBS) waiver providers and other providers of DIDD funded community services. The intent of this policy is to permit and encourage the use of electronic health records (EHRs) and electronic protected health information (EPHI), while also ensuring that providers are compliant with all applicable federal and state laws and regulations, policies and interpretive guidance, including but not limited to those referenced herein.
- III. **APPLICATION:** This policy applies to HCBS waiver providers and providers of DIDD-funded community services that elect to utilize an electronic health record and/or electronic or digital signature system for person's records and other records related to the provision of such services (e.g., personnel records, training records, and subcontracts) as they relate to management, provision, or delivery of health-related services.
- IV. **DEFINITIONS:**
 - A. **Administrative Safeguards** shall mean administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect EHR , EPHI, and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
 - B. **Center for Medicare/Medicaid Services (CMS)** shall mean the United States federal agency which administers Medicare, Medicaid, and the Children's Health Insurance Program.

Effective Date: April 1, 2016	Policy #: 80.4.4	Page 2 of 5
Subject: ELECTRONIC RECORDS AND SIGNATURES		

- C. **Digital Signature** shall mean an electronic signature, which is the result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation.
- D. **Electronic Authentication** shall mean the process of establishing confidence in user identities presented electronically to an information system in order to establish authenticity, integrity and non-repudiation.
- E. **Electronic Health Record (EHR)** shall mean an aggregate electronic record of health-related information on an individual that is created, gathered, and maintained cumulatively across one or more health care organization(s). This record may be consulted by licensed clinicians and staff involved in the individual's health and care.
- F. **Electronic Protected Health Information (EPHI)** shall mean protected health information that is transmitted by electronic media or maintained in electronic media.
- G. **Electronic Signature** shall mean a method of signing an electronic message that: identifies and authenticates a particular person as the source of the electronic message; and indicates such person's approval of the information contained in the electronic message. It may include any electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
- H. **Health Information Portability and Accountability Act (HIPAA)** shall mean the Federal law enacted by the United States Congress in 1996 to address the security and privacy of health data.
- I. **Home and Community Based Services (HCBS) Waiver or Waiver** shall mean a waiver approved for Tennessee by the Centers for Medicare and Medicaid Services to provide services to a specified number of Medicaid eligible individuals who have an intellectual disability and who meet criteria for Medicaid criteria of reimbursement in an Intermediate Care Facility for People with Intellectual Disabilities. The HCBS waivers for people with Intellectual Disabilities in Tennessee are operated by the Department of Intellectual Disabilities with oversight from TennCare, the state Medicaid agency.
- J. **Physical Safeguards** shall mean physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Effective Date: April 1, 2016	Policy #: 80.4.4	Page 3 of 5
Subject: ELECTRONIC RECORDS AND SIGNATURES		

K. **Technical Safeguards** shall mean the technology and the policy and procedures for its use that protect EHR and control access to it.

V. **POLICY:** The creation, presentation, retention, and exchange of records containing person-supported protected health information pertaining to eligibility to receive, delivery of, and payment for home and community based services are permitted in an electronic format. An electronic or digital signature is recognized as a legitimate method for authentication of an entry in the record, so long as it comports with definitions and standards set forth in federal and state law and regulation, as well as this policy.

VI. **PROCEDURES:**

A. Establishment of Electronic Health Records

1. Providers electing to maintain health information in an EHR must maintain written or electronic policies and procedures to prevent, detect, contain and correct security violations, and guide in the operations and maintenance of EHR systems to ensure information integrity, availability and security. These policies and procedures must be:
 - a. Retained for six (6) years from the date of creation or the date when last in effect, whichever is later.
 - b. Available to those persons responsible for implementing the policies and procedures.
 - c. Reviewed and updated as needed in response to environmental, legislative, or operational changes affecting the security of the EHRs.
2. EHRs are considered all or part of the person's confidential main file. EHRs must meet all standards established by federal and state law and regulation, policies and interpretive guidance.
3. EHRs must be maintained on a secure system, and all applicable administrative, physical and technical safeguards must be in place to ensure the security and privacy of all health records.
4. Required employee access to persons-supported or employee personnel file information may be accessed in a facility or service site either through a paper file system, electronic file system, or a combination of both. If records may be accessed from a residential facility, supported living site or day services facility electronically and/or printed on hard copy as needed or

Effective Date: April 1, 2016	Policy #: 80.4.4	Page 4 of 5
Subject: ELECTRONIC RECORDS AND SIGNATURES		

requested, it is not necessary to produce the information on paper until needed and/or requested, except as set forth in (5) below.

5. It is the provider's responsibility to ensure ready access to the person's information in a timely manner. If an agency utilizes EHRs as a means to store people's file information, there must be an established protocol to help ensure ready access to needed person's information in the event that technology does not function properly. As part of this protocol, providers are required to maintain a hard copy of the current Individual Support Plan in the residential facility or supported living where the person lives and in any other licensed facility where services are delivered, including day services facilities.

B. Use of Electronic and/or Digital Signatures

The acceptable use of an electronic and/or digital signature must:

1. Be unique to the user, under his or her sole control, and verify the identity of the signer (or "authenticate the user") to a person receiving or reviewing the signed record. A simple typed signature, symbol or mark does not satisfy this requirement if persons other than the signer could also have typed such signature, or provided such symbol or mark.
2. Ensure that what was signed cannot be altered. A compliant system of electronic signature must be able to detect changes to the electronic record made after it was electronically signed. Any change to the document once it has been signed invalidates the signature.
3. Provide non-repudiation, meaning that the system of electronic signature should not permit the signer to successfully deny that he willingly and intentionally signed the document, or is not responsible for information contained in the signed record. This may be accomplished, for example, through use of an acknowledgement that the user must click in order to sign the record.

C. Providers electing to utilize electronic and/or digital signatures must adopt a usage policy incorporating at a minimum, the following information:

1. Definition of electronic and/or digital signature.
2. How the provider's system of electronic and/or digital signature comports with each of the elements of acceptable use specified above.

Effective Date: April 1, 2016	Policy #: 80.4.4	Page 5 of 5
Subject: ELECTRONIC RECORDS AND SIGNATURES		

3. Acknowledgement that the electronic and/or digital signature is legally enforceable.
4. Retention of an electronic document with an electronic and/or digital signature will satisfy record retention requirements.

VII. **CQL STANDARD:** None

VIII. **REVISION HISTORY:** November 18, 2015

IX. **TENNCARE APPROVAL:** December 18, 2015

X. **ATTACHMENTS:** None